

REMARKS

New claim 7 has been added to the above-identified application. Support for claim 7 can be found throughout the Specification, e.g., on pages 2-3. No new matter has been added. Thus, claims 4 to 7 are pending now in the above-identified application.

Applicants respectfully request reconsideration of the present application in view of this response.

Regarding paragraph one (1) of the Office Action, a drawing is requested. In accordance with this request, Applicants provide the attached drawing entitled Fig. 1. The Specification has been amended in accordance with the addition of the new drawing. No new matter has been added. Support for Fig. 1 can be found in claim 4 and throughout the Specification. Accordingly, Applicants respectfully submits that the attached Fig. 1 fulfills the request of the Examiner.

Regarding paragraphs two (2) and three (3) of the Office Action, claims 4 to 6 were rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 4,868,877 to Fischer (the "Fischer reference").

The Fischer reference purportedly concerns a public key cryptographic system with enhanced digital signature certification, employing a hierarchy of nested certifications and signatures which indicate the authority and responsibility levels of the individual whose signature is being certified. Abstract, lines 1-6. The Fischer reference refers to referencing counter-signature and joint-signature requirements in each digital certification to permit business transactions to take place electronically, which heretofore would only take place after at least one party physically winded its way through a corporate bureaucracy. Abstract, lines 10-16. The Fischer reference further refers to a certifier, in constructing a certificate, generating a special message that includes fields identifying the public key which is being certified and the name of the certifiee. Abstract, lines 16-19. The Fischer reference further refers to the certificate being constructed by the certifier which includes the authority which is being granted including information which reflects issues of concern to the certifier such as, for example, the monetary limit for the certifiee and the level of trust which is granted to the certifiee. Abstract, lines 19-24.

Independent claim 4 concerns a method for generating, personalizing, and certifying an asymmetrical cryptokey in accordance with one of an operation performed at a central,

secure location correspondence to a trust center and an operation performed at a user location in cooperation with the trust center using a secure transmission between a user and the trust center, and recites:

- causing the trust center to provide the user with a previously generated, personalized, and certified signature key pair, and with components for producing at least one encryption key pair;

- producing the at least one encryption key pair including a public part and a secret part;

- marking the public part of the at least one encryption key pair using an assigned secret part of the previously generated signature key pair;

- after marking the public part of the at least one encryption key pair, transmitting the at least one encryption key pair to the trust center;

- unequivocally assigning the at least one encryption key pair to the user;

- causing the trust center to check the unequivocal assignment of the at least one encryption key pair by using a public part of the previously generated signature key pair;

- after the check of the unequivocal assignment is performed successfully, causing the trust center to produce a new certificate by using at least one of the public part of the previously generated signature key pair and the public part of the at least one encryption key pair;

- encrypting the new certificate using the public part of the at least one encryption key pair; and

- causing the trust center to transmit the encrypted new certificate to the user.

In contrast, the Fischer reference does not *identically* disclose (as it must for anticipation) or suggest at least the features of *producing the at least one encryption key pair* including a public part and a secret part; *marking the public part of the at least one encryption key pair using an assigned secret part of the previously generated signature key pair*; after marking the public part of the at least one encryption key pair, transmitting the at least one encryption key pair to the trust center; unequivocally assigning the at least one encryption key pair to the user; *causing the trust center to check the unequivocal assignment of the at least one encryption key pair by using a public part of the previously generated signature key pair*; after the check of the unequivocal assignment is performed successfully, *causing the trust center to produce a new certificate by using at least one of the public part of the previously generated signature key pair and the public part of the at least one encryption key pair*; *encrypting the new certificate using the public part of the at least one encryption key pair*, as claimed in claim 4. Instead, the Fischer reference refers to a user digitally signing a purchase order under the authority of a certificate appended to the transmitted message – a

message can be signed by applying to it at least a portion of the object being signed, the privately held signature key. Col. 7, lines 5-11. The Fischer reference further states that by signing an image of the object or a more compact version thereof known as a digest or hash of the object, with the secret key, it is possible for anyone with access to the public key to encrypt the result and compare it with the object or a recomputed hash or digit version thereof. Col. 7, lines 11-17. The Fischer reference further states that because only the owner of the public key could have used the secret key to perform this operation, the owner of the public key is thereby confirmed to have signed the message. Col. 7, lines 17-20. The Fischer reference states that a digital signature is accompanied by at least one valid certificate which specifies the identity of the signer and the authorization which the signer has been granted – to be valid, a certificate must be signed by the private key associated with one or more other valid certificates. Col. 7, lines 20-33. The Fischer reference indicates that one or more other valid certificates must grant the signer the authority to create such a signature and/or to issue the purchase order. Col. 7, lines 33-36. The Fischer reference further states that any party who receives a message transmitted by the user can verify and validate the user's signature and the authority that the user exercised, such validation being possible since a complete hierarchy of validating certificates is transmitted with the original purchase order which permits the ultimate recipient to feel confident that the requested transaction is authentic and properly authorized. Col. 7, line 61 - col. 8, line 3.

Accordingly, the Fischer reference does not render obvious claim 4, and withdrawal of the rejection of claim 4 under 35 U.S.C. § 102 (b) is respectfully requested.

Since claims 5 and 6 depend from claim 4, claims 5 and 6 are allowable for at least the same reasons as claim 4.

Accordingly, the Fischer reference does not identically disclose or even suggest the features of claim 4. Withdrawal of the rejection of claims 4 to 6 under 35 U.S.C. § 102(b) is respectfully requested.

New claim 7 contains analogous features to claim 4; accordingly, it is respectfully submitted that claim 7 is also allowable over the art cited in the Office Action for essentially the same reasons as for claim 4. No new matter has been added.

In summary, it is respectfully submitted that all of claims 4 to 7 of the above-identified application are allowable for the foregoing reasons.

CONCLUSION

In view of all of the above, it is believed that the rejections of claims 4 to 6 have been obviated. Accordingly, it is respectfully submitted that all claims 4 to 7 are allowable.

It is therefore respectfully requested that the rejections be reconsidered and withdrawn, and that the present application issue as early as possible.

If it would further allowance of the present application, the Examiner is invited to contact the undersigned.

Respectfully submitted,

Dated: Sept. 19, 2003

By: Richard L. Mayer
Richard L. Mayer
(Reg. No. 22,490)

By: Quincy J. Study
Reg. No. 47084

CUSTOMER NO. 26646

KENYON & KENYON
One Broadway
New York, New York 10004
(212) 425-7200